IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	)	
	)	
Huayan Wang et al.	)	
	)	
Serial No.: 10/026,043	)	Group Art Unit: 2132
	)	
Filed: October 25, 2001	)	Examiner: Jung W. Kim
	)	
For: SYSTEM AND METHOD FOR	)	**Board of Patent Appeals and**
UPPER LAYER ROAMING	)	**Interferences**
AUTHENTICATION	)	
	)	

Mail Stop: Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

In support of the Notice of Appeal filed on August 1, 2008, and pursuant to 37 C.F.R. § 41.37, Appellants present this appeal brief in the above-captioned application.

This is an appeal to the Board of Patent Appeals and Interferences from the Examiner's final rejection of claims 1-21 in the Final Office Action dated May 14, 2008. The appealed claims are set forth in the attached Claims Appendix.

1.   Real Party in Interest

        This application is assigned to Symbol Technologies, Inc., which has merged with
Motorola, Inc., the real party in interest.

2.   Related Appeals and Interferences

        There are no other appeals or interferences which would directly affect, be
directly affected, or have a bearing on the instant appeal.

3.   Status of the Claims

        Claims 1-21 have been rejected in the Final Office Action. The final rejection of
claims 1-21 is being appealed.

4.   Status of Amendments

        All amendments submitted by Appellants have been entered.

5.   Summary of Claimed Subject Matter

        The present invention, recited in an independent claim 1, relates to a method for
authenticating a roaming device with a network. (See Specification, Fig. 2). The method
generates (202), by an authentication server (10) of the network (18), authentication data
associated with the roaming device (20). (See Id., p. 4, l. 29 – p. 5, l. 1; p. 6, ll. 17-19; Figs. 1-2).
The method sends (204), by the authentication server (10), the authentication data to access
points (12, 14, 16) of the network (18). (See Id., p. 5, ll. 6-8; p. 6, ll. 19-24; Figs. 1-2). The
access points (12, 14, 16) are connected to the authentication server (10). (See Id., p. 4, ll. 12-14;
Fig. 1). When the roaming device (20) roams to a particular access point (12, 16) of the access
points (12, 14, 16), the method determines if the particular access point (12, 16) has
authentication data associated with the roaming device (20) and uses (208-216) the
authentication data to locally authenticate the roaming device (20) at the particular access point
(12, 16) if the determination is positive. (See Id., p. 7, l. 19 – p. 8, l. 20; Figs. 1-2). If the
determination is negative, the authentication process is carried out at the authentication server
(10) if the determination is negative. (See Id., p. 6, ll. 2-5; Figs. 1-2).

The present invention, recited in an independent claim 10, relates to a method for authenticating a roaming device with a network. (See Specification, Fig. 2). The method connects (202) the roaming device (20) with an authentication server (10) upon a contact of the roaming device (20) with a first access point (14) of the network (18). (See Id., p. 4, ll. 19-22; p. 6, ll. 17-19; Figs. 1-2). The method authenticates (206) the roaming device (20) with the authentication server (10) if the access point (14) has no authentication data associated with the roaming device (20). (See Id., p. 6, ll. 2-5, 18-19; Figs. 1-2). The method generates (202) authentication data for the roaming device (20). (See Id., p. 4, l. 29 – p. 5, l. 1; p. 6, ll. 17-19; Figs. 1-2). The method distributes (204), by the authentication server (10), the authentication data to the first access point (14) and a second access point (12 or 16) of the network (18). (See Id., p. 5, ll. 6-8; p. 6, ll. 19-24; Figs. 1-2). The method locally authenticates (208-216) the roaming device (20) upon a contact with the second access point (12 or 16) using the distributed authentication data. (See Id., p. 7, l. 19 – p. 8, l. 20; Figs. 1-2).

The present invention, recited in an independent claim 16, relates to a system for authenticating a roaming device with a network. (See Id., Fig. 1). The system comprises an authentication server (10) connected to the network (18). (See Id., p. 4, ll. 11-17; Fig. 1). The system also comprises first (14) and second (12 or 16) access points connected to the authentication server (10). (See Id.). The first (14) and second (12 or 16) access points are capable of communicating with the roaming device (20). (See Id., p. 4, ll. 19-24; Fig. 1). Each of the first (14) and second (12 or 16) access points include a memory arrangement capable of storing authentication data corresponding to the roaming device (20). (See Id., p. 7, ll. 3-4; Fig. 1). The authentication server (10) sends (204) the authentication data to the first (14) and second (12 or 16) access points upon an initial authentication procedure of the roaming device (20) with the first access point (14) when the first access point (14) has no authentication data associated with the roaming device (20). (See Id., p. 5, ll. 6-8; p. 6, ll. 2-5, 19-24; Figs. 1-2). The second access point (12 or 16) locally authenticates (208-216) the roaming device (20) upon a contact of the roaming device (20) with the second access point (12 or 16). (See Id., p. 7, l. 19 – p. 8, l. 20; Figs. 1-2).

The present invention, recited in an independent claim 19, relates to a method for authenticating a roaming device with a network. (See Id., Fig. 2). With an authentication server (10), the method receives (202) an authentication request (802.11 Probe/Probe Response) from

the roaming device (20) if the access point (12, 14, 16) connected with the roaming device (20) has no authentication data associated with the roaming device (20). (See Id., p. 4, ll. 19-22; p. 6, ll. 2-5, 17-19; Figs. 1-3). The request is encrypted with a first shared code. (See Id., p. 10, ll. 1-3). With the authentication server (10), the method generates (202) a session key (EAP Identity) associated with the roaming device (20). (See Id., p. 4, l. 29 – p. 5, l. 1; p. 6, ll. 17-19; Figs. 1-2). The method sends (204) the session key (EAP Identity) to an access point (12, 14, 16) of the network (18). (See Id., p. 5, ll. 6-8; p. 6, ll. 19-24; Figs. 1-2). The session key (EAP Identity) is encrypted with a second shared code. (See Id., p. 10, ll. 7-9). The method utilizes (208-216) the session key (EAP Identity) to authenticate the roaming device (20) at the access point (12, 14, 16) and to encrypt data exchanged between the roaming device (20) and the access point (12, 14, 16). (See Id., p. 7, l. 19 – p. 8, l. 20; p. 10, ll. 9-12; Figs. 1-2).

6.   Grounds of Rejection to be Reviewed on Appeal

I.   Whether claims 1-3, 6, 10, 11, and 15-18 are unpatentable under 35 U.S.C. § 103(a) over U.S. Pat. No. 6,760,444 to Leung in view of U.S. Pat. No. 5,732,350 to Marko et al. (hereinafter "Marko").

II.   Whether claims 4-5 are unpatentable under 35 U.S.C. § 103(a) over Leung in view of Marko in further view of U.S. Pat. No. 5,408,683 to Ablay et al. (Ablay).

III.   Whether claims 7, 8, and 13 are unpatentable under 35 U.S.C. § 103(a) over Leung in view of Marko in further view of U.S. Pat. No. 6,452,910 to Vij et al. (Vij).

IV.   Whether claims 9, 12, and 14 are unpatentable under 35 U.S.C. § 103(a) over Leung in view of Marko in further view of U.S. Pat. Application No. 2002/0174335 to Zhang et al. (hereinafter "Zhang").

V.   Whether claim 19 is unpatentable under 35 U.S.C. § 103(a) over Leung in view of Zhang.

4

VI.   Whether claim 20 is unpatentable under 35 U.S.C. § 103(a) over Leung in view of Zhang in further view of Marko.

VII.   Whether claim 21 is unpatentable under 35 U.S.C. § 103(a) over Leung in view of Zhang in further view of U.S. Pat. No. 6,178,506 to Quick, Jr. (hereinafter "Quick").

7.   Argument

I.   The Rejection of Claims 1-3, 6, 10, 11, and 15-18 Under 35 U.S.C. § 103(a) Over Leung in view of Marko Should Be Reversed.

A.   The Examiner's Rejection

In the Final Office Action, the Examiner rejected claims 1-3, 6, 10, 11, and 15-18 under 35 U.S.C. § 103(a) as being unpatentable over Leung in view of Marko. (See 5/14/08 Office Action, p. 3).

Leung discloses a method for authenticating a roaming device with a network, comprising the steps of generating by an authentication server of the network, authentication data associated with the roaming device, sending the authentication data to a Home Agent of the network which is connected to the authentication server, and using the authentication data to locally authenticate the roaming device at the particular access point. (See Leung Abstract).

Marko discloses a method for registering a mobile station among a plurality of base stations defined by a cell grouping level based upon a dynamic algorithm, when the base station registers with an initial base station and the base station provides a cell grouping level. (See Marko Abstract).

B.   The Cited Patents Do Not Disclose or Suggest Determining If the Particular Access Point Has Authentication Data Associated with the Roaming Device, Using the Authentication Data to Locally Authenticate the Roaming Device at the Particular Access Point If the Determination Is Positive, or Carrying Out the Authentication Process at the Authentication Server If the Determination Is Negative, as recited in claim 1.

In the claimed invention, the access point, upon being contacted by a mobile station, first determines whether a WEP-session key has already been generated for the mobile

5

station by the authentication server and been broadcasted to the access points within the ESS, and then the authentication process will diverge based on the determination result. (See Specification [0018]-[0023]). If a WEP-session key associated with the mobile station has already been generated and stored in the access point, the access point will start to perform the authentication process locally. (See Specification [0021], [0022]). On the other hand, if the WEP-session key has not been generated, the authentication process will take place in the authentication server, then the WEP key will be sent to the current access point connected to the mobile station and also the additional access points in the ESS. (See Specification [0018]).

However, it is clear that the system in Leung does not perform the above-mentioned step to determine where the authentication procedure will take place. Specifically, the authentication of the mobile node in Leung can be performed either by the server which provides a plurality of security associations for a plurality of mobile nodes, or by the Home Agent locally. (See Leung Abstract, Fig. 7, Fig. 8). Nevertheless, where to perform the authentication is not triggered by any particular condition, such as the Home Agent's determining if it has the authentication data associated with the mobile node, but is configured according to the preference of the network operator. (See Leung col. 8, line 13-25). Indeed, the Home Agent in both these two embodiments of the devices only checks the mobile node list stored on the Home Agent to identify which authentication server handles security associations for the particular mobile node making the registration request, then sends out different packet data to the server based on the operational preference. (See Fig. 7, Fig. 8, col. 7, line 10-30, col. 8, line 30-50).

The Examiner appears to reply to the above argument with a narrow embodiment that is possible in Leung. Specifically, the Examiner states that "there exists a third scenario in Leung's disclosure: when a mobile node moves from a foreign agent to the home agent. In this scenario, the home agent will have a cached value of the authentication data because the home agent caches the authentication data when it receives an authentication request from a foreign agent from the mobile node-the mobile node came from a foreign agent, hence, an earlier authentication request was submitted via the foreign agent to the home agent." (See 7/28/08 Advisory Action, p. 2, ll. 7-13). However, it is respectfully submitted that the recitation of claim 1 explicitly precludes the scenario to which the Examiner refers. That is, claim 1 explicitly differentiates between the authentication server and the access points. The Examiner analogizes

the authentication server of claim 1 to the Home Agent of Leung. Claim 1 further explicitly recites "when the roaming device roams to a particular access point of the access points." That is, claim 1 refers to when the roaming device roams into an operating area that is *not* managed by the authentication server. The third scenario referenced by the Examiner specifically relates to when the roaming device roams into an operating area of the Home Agent. Therefore, it is respectfully submitted that the Examiner's narrow interpretation of Leung is misplaced and does not obviate the recitation of claim 1. It is also noted that it appears that the Examiner implies that the first and second scenarios referenced above are not obviated by Leung since the Examiner only relies upon the third scenario.

Marko also does not overcome this deficiency described regarding Leung.

Thus, it is respectfully submitted that neither Leung nor Marko, either alone or in combination, discloses or suggests "determining if the particular access point has authentication data associated with the roaming device, using the authentication data to locally authenticate the roaming device at the particular access point if the determination is positive, or carrying out the authentication process at the authentication server if the determination is negative," as recited in claim 1. Accordingly, it is respectfully submitted that claims 1 and all depending claims (claims 2, 3, and 6) are allowable.

Claim 10 recites "authenticating the roaming device with the authentication server if the access point has no authentication data associated with the roaming device," "distributing the authentication data to the first access point and a second access point of the network ," and "locally authenticating the roaming device upon a contact with the second access point using the distributed authentication data." Claim 16 recites "wherein the authentication server sends the authentication data to the first and second access points upon an initial authentication procedure of the roaming device with the first access point when the first access point has no authentication data associated with the roaming device," and "wherein the second access point locally authenticates the roaming device upon a contact of the roaming device with the second access point." Thus, it is respectfully submitted that claims 10, 16 and all depending claims (claims 11, 15, 17, and 18) are allowable.

7

II.   The Rejection of Claims 4-5 Under 35 U.S.C. § 103(a) Over Leung in view of
        Marko in further view of Ablay Should Be Reversed.

        A.   The Examiner's Rejection

        In the Final Office Action, the Examiner rejected claims 4-5 under 35 U.S.C. §

103(a) as being unpatentable over Leung in view of Marko in further view of Ablay. (See

5/14/08 Office Action, p. 10). Leung and Marko were discussed above.

        Ablay is directed toward tracking subscribers in a networked radio

communications system. The subscribers are able to roam among a plurality of coverage areas

which are serviced by a plurality of transmitters. The transmitters are coupled to a central

processor which access a memory device for storing subscriber records and site records. The

method relies on the subscriber sending an inbound message which includes its current location.

(See Ablay, abstract). Ablay does not include any disclosure concerning a local authentication

for the subscribers at the plurality of transmitters.

        B.   The Cited Patents Do Not Disclose or Suggest Determining If the
                Particular Access Point Has Authentication Data Associated with the
                Roaming Device, Using the Authentication Data to Locally Authenticate
                the Roaming Device at the Particular Access Point If the Determination Is
                Positive, or Carrying Out the Authentication Process at the Authentication
                Server If the Determination Is Negative, as recited in claim 1.

        As discussed above, neither Leung nor Marko, either alone or in combination,

discloses or suggests "determining if the particular access point has authentication data

associated with the roaming device, using the authentication data to locally authenticate the

roaming device at the particular access point if the determination is positive, or carrying out the

authentication process at the authentication server if the determination is negative," as recited in

claim 1. Ablay also does not disclose or suggest this recitation of claim 1. Thus, neither Leung,

Marko, nor Ablay, either alone or in combination, discloses or suggests this recitation of claim 1.

Because claims 4-5 depend from and, therefore, include the limitations of claim 1, it is

respectfully submitted that these claims are also allowable.

III.   The Rejection of Claims 7, 8 and 13 Under 35 U.S.C. § 103(a) Over Leung in view of Marko in further view of Vij Should Be Reversed.

A.   The Examiner's Rejection

In the Final Office Action, the Examiner rejected claims 7, 8 and 13 under 35 U.S.C. § 103(a) as being unpatentable over Leung in view of Marko in further view of Vij. (See 5/14/08 Office Action, p. 11). Leung and Marko were discussed above.

Vij is directed toward a wireless bridge that connects two previously incompatible technologies within a single device to leverage the strengths of each. The wireless bridge marries a personal area network technology with a wireless local area network to provide a wireless system for peripheral devices. (See Vij, abstract). Vij concerns the separation and shielding required of potentially conflicting technologies to inter-operate. That is, there is no disclosure in Vij concerning a local authentication for a roaming device at a particular access point.

B.   The Cited Patents Do Not Disclose or Suggest Determining If the Particular Access Point Has Authentication Data Associated with the Roaming Device, Using the Authentication Data to Locally Authenticate the Roaming Device at the Particular Access Point If the Determination Is Positive, or Carrying Out the Authentication Process at the Authentication Server If the Determination Is Negative, as recited in claim 1.

As discussed above, neither Leung nor Marko, either alone or in combination, discloses or suggests "determining if the particular access point has authentication data associated with the roaming device, using the authentication data to locally authenticate the roaming device at the particular access point if the determination is positive, or carrying out the authentication process at the authentication server if the determination is negative," as recited in claim 1. Vij also does not disclose or suggest this recitation of claim 1. Thus, neither Leung, Marko, nor Vij, either alone or in combination, discloses or suggests this recitation of claim 1. Because claims 7, 8, and 13 depend from and, therefore, include the limitations of allowable claims, it is respectfully submitted that these claims are also allowable.

IV. The Rejection of Claims 9, 12, and 14 Under 35 U.S.C. § 103(a) Over Leung in view of Marko in further view of Zhang Should Be Reversed.

A. The Examiner's Rejection

In the Final Office Action, the Examiner rejected claim 9 under 35 U.S.C. § 103(a) as being unpatentable over Leung in view of Marko in further view of Zhang. (See 5/14/08 Office Action, p. 13). Leung and Marko were discussed above.

Zhang is directed toward converging both the authentication, accounting, and authorization process with data transmissions at the Internet Protocol layer. (See Zhang, abstract). Zhang still maintains a communication with the access point to an authentication server to authenticate mobile devices. That is, there is no disclosure in Zhang concerning a local authentication for a roaming device at a particular access point.

B. The Cited Patents Do Not Disclose or Suggest Determining If the Particular Access Point Has Authentication Data Associated with the Roaming Device, Using the Authentication Data to Locally Authenticate the Roaming Device at the Particular Access Point If the Determination Is Positive, or Carrying Out the Authentication Process at the Authentication Server If the Determination Is Negative, as recited in claim 1.

As discussed above, neither Leung nor Marko, either alone or in combination, discloses or suggests "determining if the particular access point has authentication data associated with the roaming device, using the authentication data to locally authenticate the roaming device at the particular access point if the determination is positive, or carrying out the authentication process at the authentication server if the determination is negative," as recited in claim 1. Zhang also does not disclose or suggest this recitation of claim 1. Thus, neither Leung, Marko, nor Zhang, either alone or in combination, discloses or suggests this recitation of claim 1. Because claims 9, 12, and 14 depend from and, therefore, include the limitations of allowable claims, it is respectfully submitted that these claims are also allowable.

V.   The Rejection of Claim 19 Under 35 U.S.C. § 103(a) Over Leung in view of <u>Zhang Should Be Reversed.</u>

A.   <u>The Examiner's Rejection</u>

In the Final Office Action, the Examiner rejected claim 19 under 35 U.S.C. § 103(a) as being unpatentable over Leung in view of Zhang. (<u>See</u> 5/14/08 Office Action, p. 16). Leung and Zhang were discussed above.

B.   The Cited Patents Do Not Disclose or Suggest With an Authentication Server, Receiving an Authentication Request From a Roaming Device If the Access Point Connected With the Roaming Device Has No Authentication Data Associated With the Roaming Device and Utilizing the Session Key to Authenticate the Roaming Device at the Access Point, <u>as recited in claim 19.</u>

As discussed above, neither Leung nor Zhang, either alone or in combination, discloses or suggests "determining if the particular access point has authentication data associated with the roaming device, using the authentication data to locally authenticate the roaming device at the particular access point if the determination is positive, or carrying out the authentication process at the authentication server if the determination is negative," as recited in claim 1. Claim 19 recites "with an authentication server, receiving an authentication request from a roaming device if the access point connected with the roaming device has no authentication data associated with the roaming device," and "utilizing the session key to authenticate the roaming device at the access point." Thus, it is respectfully submitted that neither Leung nor Zhang, either alone or in combination, discloses or suggests this recitation of claim 19 and, therefore, claim 19 is allowable.

VI.   The Rejection of Claim 20 Under 35 U.S.C. § 103(a) Over Leung in view of <u>Zhang in further view of Marko Should Be Reversed.</u>

A.   <u>The Examiner's Rejection</u>

In the Final Office Action, the Examiner rejected claim 20 under 35 U.S.C. § 103(a) as being unpatentable over Leung in view of Zhang in further view of Marko. (<u>See</u> 5/14/08 Office Action, p. 17). Leung, Zhang, and Marko were discussed above.

11

B.   The Cited Patents Do Not Disclose or Suggest With an Authentication Server, Receiving an Authentication Request From a Roaming Device If the Access Point Connected With the Roaming Device Has No Authentication Data Associated With the Roaming Device and Utilizing the Session Key to Authenticate the Roaming Device at the Access Point, <u>as recited in claim 19.</u>

As discussed above, neither Leung nor Zhang, either alone or in combination, discloses or suggests "with an authentication server, receiving an authentication request from a roaming device if the access point connected with the roaming device has no authentication data associated with the roaming device," and "utilizing the session key to authenticate the roaming device at the access point," as recited in claim 19. Also as discussed above, Marko does not disclose or suggest a substantially similar recitation of claim 1. Thus, neither Leung, Zhang, nor Marko, either alone or in combination, discloses or suggests this recitation of claim 19. Because claim 20 depends from and, therefore, includes all the limitations of claim 19, it is respectfully submitted that this claim is also allowable.

VII.   The Rejection of Claim 21 Under 35 U.S.C. § 103(a) Over Leung in view of <u>Zhang in further view of Quick Should Be Reversed.</u>

A.   <u>The Examiner's Rejection</u>

In the Final Office Action, the Examiner rejected claim 21 under 35 U.S.C. § 103(a) as being unpatentable over Leung in view of Zhang in further view of Quick. (See 5/14/08 Office Action, p. 18). Leung and Zhang were discussed above.

Quick is directed toward a pin identification number to transfer a subscription for wireless service to a new wireless terminal. (See Quick, abstract). Quick concerns a subscription at the mobile device level and incorporates conventional authentication procedures where the access point communicates with an authentication server to authenticate the mobile device. That is, there is no disclosure in Quick concerning a local authentication for a roaming device at a particular access point.

B.   The Cited Patents Do Not Disclose or Suggest With an Authentication Server, Receiving an Authentication Request From a Roaming Device If the Access Point Connected With the Roaming Device Has No Authentication Data Associated With the Roaming Device and Utilizing the Session Key to Authenticate the Roaming Device at the Access Point, <u>as recited in claim 19.</u>

As discussed above, neither Leung nor Zhang, either alone or in combination, discloses or suggests "with an authentication server, receiving an authentication request from a roaming device if the access point connected with the roaming device has no authentication data associated with the roaming device," and "utilizing the session key to authenticate the roaming device at the access point," as recited in claim 19. Quick also does not disclose or suggest this recitation of claim 19. Thus, neither Leung, Zhang, nor Quick, either alone or in combination, discloses or suggests this recitation of claim 19. Because claim 21 depends from and, therefore, includes the limitations of claim 19, it is respectfully submitted that this claim is also allowable.
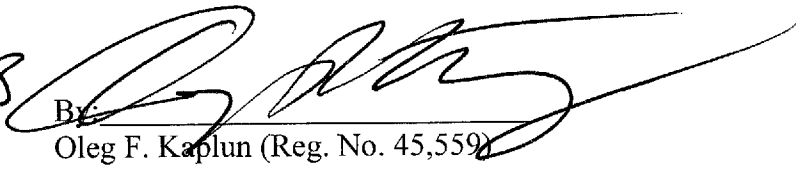
8.   Conclusion

For the reasons set forth above, Appellants respectfully request that the Board reverse the rejection of the claims by the Examiner under 35 U.S.C. § 103(a), and indicate that claims 1-21 are allowable.

Respectfully submitted,

Date: _Sept 30,2008_   By: _____
Oleg F. Kaplun (Reg. No. 45,559)

Fay Kaplun & Marcin, LLP
150 Broadway, Suite 702
New York, NY 10038
Tel: (212) 619-6000
Fax: (212) 619-0276

CLAIMS APPENDIX

1.   (Previously Presented) A method for authenticating a roaming device with a network, comprising the steps of:

generating, by an authentication server of the network, authentication data associated with the roaming device;

sending the authentication data to access points of the network, the access points being connected to the authentication server; and

when the roaming device roams to a particular access point of the access points, determining if the particular access point has authentication data associated with the roaming device, using the authentication data to locally authenticate the roaming device at the particular access point if the determination is positive, or carrying out the authentication process at the authentication server if the determination is negative.

2.   (Original) The method according to claim 1, further comprising the step of:

storing the authentication data in a memory arrangement of each of the access points.

3.   (Original) The method according to claim 1, wherein the sending step includes the substeps of:

encrypting the authentication data; and

sending the encrypted authentication data to selected access points of the access points.

4.   (Original) The method according to claim 3, wherein the sending step includes the substeps of:

determining at least one access point of the access points using prediction algorithms to anticipate where the roaming device will roam; and

sending the encrypted authentication data to the at least one access point.

5.   (Original) The method according to claim 3, wherein the sending step includes the substep of sending the encrypted authentication data to all the access points.

6.   (Original) The method according to claim 1, further comprising the preliminary steps of:

determining if the particular access point has authentication data associated with the roaming device;

if the determination is positive, proceed to the step of using the authentication data to locally authenticate the roaming device at the particular access point; and

if the determination is negative, proceed to the step of generating, by an authentication server of the network, authentication data associated with the roaming device.

7.   (Original) The method according to claim 6, wherein the step of using the authentication data to locally authenticate the roaming device further comprises reassociating the roaming device with the particular access point of the access points by exchanging identification information.

8.   (Original) The method according to claim 7, wherein the reassociating step further includes the substeps of:

searching a memory arrangement of the particular access point for the authentication data associated with the roaming device; and

if the authentication data is found, performing a mutual authentication procedure between the roaming device and the particular access point.

9.   (Original) The method according to claim 1, wherein the generating step further includes the steps of:

receiving an encrypted authentication request from the roaming device;

determining that the roaming device can be granted access to network services; and

generating an encrypted session key associated with the roaming device in the authentication server.

10.   (Previously Presented) A method for authenticating a roaming device with a network, comprising the steps of:

connecting the roaming device with an authentication server upon a contact of the roaming device with a first access point of the network;

16

authenticating the roaming device with the authentication server if the access point has no authentication data associated with the roaming device;

generating authentication data for the roaming device;

distributing the authentication data to the first access point and a second access point of the network; and

locally authenticating the roaming device upon a contact with the second access point using the distributed authentication data.

11. (Original) The method according to claim 10, further comprising the step of:

authenticating the roaming device with the authentication server if the local authentication of the roaming device fails.

12. (Original) The method according to claim 10, wherein the distributing step further includes the substep of:

distributing an encrypted session key to the first and second access points.

13. (Original) The method according to claim 10, wherein the locally authenticating step further includes the substeps of:

exchanging identification data between the roaming device and the second access point; and

correlating the identification data with the distributed authentication data.

14. (Original) The method according to claim 10, further comprising the step of:

establishing a shared secret encryption between the authentication server and the first and second access points.

15. (Original) The method according to claim 10, wherein the authentication server is a remote authentication dial-in user server.

16. (Previously Presented) A system for authenticating a roaming device with a network, comprising:

an authentication server connected to the network; and

first and second access points connected to the authentication server, the first and second access points being capable of communicating with the roaming device, each of the first and second access points including a memory arrangement capable of storing authentication data corresponding to the roaming device,

wherein the authentication server sends the authentication data to the first and second access points upon an initial authentication procedure of the roaming device with the first access point when the first access point has no authentication data associated with the roaming device, and

wherein the second access point locally authenticates the roaming device upon a contact of the roaming device with the second access point.

17.   (Original) The system according to claim 16, wherein the second access point authenticates the roaming device with the authentication server if the authentication data is not found in the memory arrangement of the second access point.

18.   (Original) The system according to claim 16, wherein the second access point authenticates the roaming device with the authentication server if the local authentication of the roaming device at the second access point fails.

19.   (Previously Presented) A method for authenticating a roaming device with a network, comprising the
steps of:

with an authentication server, receiving an authentication request from a roaming device if the access point connected with the roaming device has no authentication data associated with the roaming device, the request being encrypted with a first shared code;

with the authentication server, generating a session key associated with the roaming device;

sending the session key to an access point of the network, the session key being encrypted with a second shared code; and

utilizing the session key to authenticate the roaming device at the access point, and to encrypt data exchanged between the roaming device and the access point.

20.   (Original) The method according to claim 19, further comprising the step of:

sending the encrypted session key to a further access point of the network to authenticate the roaming device at the further access point.

21.   (Original) The method according to claim 19, further comprising the steps of:

generating a first key of the session key to perform authentication of the roaming device at the access point; and

generating a second key of the session key to encrypt data exchanges between the roaming device and the access point, the second key being different from the first key.

EVIDENCE APPENDIX

No evidence has been entered or relied upon in the present appeal.

RELATED PROCEEDING APPENDIX

No decisions have been rendered regarding the present appeal or any proceedings related thereto.